Purpose

Dublin City University Educational Trust (DCUET), as a Data Controller, is required by law to comply with the following Irish legislation relating to the processing of Personal Data:

. The Data Protection Act 1988 (The Principle Act) and
. The Data Protection (Amendment) Act 2003

This document is DCUET’s policy in response to the requirements of the Data Protection Acts and provides additional guidance on the handling and security of data.

Scope

In order to carry out its fundraising, development and administrative functions DCUET needs to collect and process personal information relating to many categories of people, including alumni, students and staff of the University and non-alumni potential donors and supporters of the University’s work.

DCUET takes the confidentiality of all personal information seriously and consequently takes all reasonable steps to comply with the principles of the Data Protection Acts. DCUET aims to collect personal information only in order to meet specific legitimate purposes, and to retain that information only for as long as those purposes remain valid. Ordinarily, DCUET will not pass personal information to any third party, except where required by law, statutory obligations or legitimate purposes balanced against the rights and interests of the data subject.

DCUET is committed to ensuring that all employees, agents, contractors and data processors comply with the Data Protection Acts regarding:

- the processing and confidentiality of any personal data held by DCUET, and
- the privacy rights of individuals under the legislation.

Data Protection Principles

To comply with the law, personal data (as defined by the Data Protection Acts) must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, DCUET must comply with the following eight Data Protection Principles or Obligations:

1. Obtain and process information fairly

The Data must be obtained and processed fairly and lawfully and only when certain conditions are met. (See Definition for details on conditions regarding Personal Data and Sensitive Personal Data.)

2. Keep it only for one or more specific, explicit and lawful purposes

The Data can only be obtained for specified, lawful and clearly stated purposes.
3. Use and disclose only in ways compatible with these purposes

Processing and Disclosure of personal data should not be incompatible with the specified purpose for which it was obtained.

4. Keep it safe and secure

The Data must be kept safe and secure. DCUET, as the Data Controller, is responsible for applying adequate security structures to prevent unlawful or inadvertent processing, alteration or loss of the data.

5. Keep it accurate, complete and up-to-date

The Data must be kept accurate, complete and where necessary up-to-date.

6. Ensure it is adequate, relevant and not excessive

The Data obtained should be adequate, relevant and not excessive. Keep only the minimum amount of personal data needed for the purpose for which it is being processed.

7. Retain for no longer than is necessary

Personal data can only be held so long as there is a continuing and legitimate business use for it. Such data cannot be held on a “just-in-case” basis that a use, as yet undetermined, may be found for it in the future.

Further information on DCUET’s retention policy can be found in DCUET’s Personal Data Security Schedule (PDSS).

8. Give a copy of his/her personal data to that individual, on request

The Data Subject, the person to whom the information relates, has a Right of Access. Requests must be made in writing and a fee of up to €6.35 can be charged. The Controller must store and maintain the data in such a manner as to be able to respond to a Subject Access Request as soon as possible and within no more than 40 days.

**Disclosure of Personal Data**

The legislation recognises two categories of Personal Data –

‘Ordinary’ Personal Data relates to identifiable living individuals:

“data relating to an individual who can be identified either from the data alone or from the data in conjunction with other information that is in or is likely to come into the possession of the data controller”.

Examples of Personal Data include: name, address, mobile phone number, car registration, PPS Number.
Sensitive Personal Data, which is more deeply personal to an individual, such as their racial or ethnic background, political opinions, religious or similar beliefs, trade union membership, physical or mental health, sexual life, the (alleged) commission of any offence, subsequent proceedings or sentence.

Sensitive personal data should normally only be processed if the data subjects have given their explicit consent to this processing.

The legislation applies equally to automated and manual data, i.e. data held or processed on a computer, or data held in ‘hard copy’, stored in an indexed or relevant filing system.

Different standards are applied to publically available sensitive personal data which has been made public by the individual and that which has been made public without the consent of the individual. The latter must not be used without due consideration for the purpose for which it is being held.

The security of personal data in the possession of DCUET and the wider University is of paramount importance and is, therefore, addressed in various policies and procedures throughout the University. In addition to the principles contained within this policy, staff are also advised to read and adhere to the University’s Data Classification Policy, Data Handling Guidelines and Contact with Third Parties Policy.

All staff have an individual responsibility to ensure that they adhere to DCUET’s Data Protection Policy, the DCUET Personal Data Security Schedule and the Data Protection Acts.

Personal data should not be disclosed or transferred to a third party for any form of processing or use without putting in place a formal contract to safeguard data. The same principles apply even if the third party is to be given access to personal data within DCUET’s office or control. The University’s Data Protection Officer should be consulted if these types of arrangement are being contemplated.

**Information held by the DCU Educational Trust and Alumni Relations Office**

DCU Educational Trust and the Alumni Relations Office have a shared interest in and co-ordinated approach to our alumni and supporters. The Alumni Relations office keeps in touch with alumni and provides services to them, while DCUET focuses on relationships with potential and existing donors. Paper records are also held.

The records are used by the two offices for alumni relations and fundraising purposes. These include publications, alumni surveys, appeals and the marketing of alumni events and services such as alumni email and online services and merchandise. Communications may be sent by post, telephone or, increasingly, electronic means.

Electronic records of alumni, donors and potential supporters of DCU are held in a secure database managed by DCU’s ISS department, following industry good practice. Most records contain education, contact details and career and other achievements. Contact and relationships with the University since graduation and donations are also recorded. In some cases other data is added: data from partners
(e.g. wealth screening), sensitive data provided by individuals for a specific purpose (for example disability or lifestyle status for event management or updating of personal history), information about partners, financial and personal data from reputable public sources and references to individual’s areas of interest and potential to support the University.

All information is held and transmitted securely and (in addition to disclosure as permitted or required by law) may be disclosed on a considered and confidential basis on to:
- DCU departments and faculties
- Alumni societies and volunteers
- External suppliers acting on behalf of DCUET or the Alumni Relations

Where an external party needs to have access to, or to obtain data from DCUET, then a formal data protection contract must be signed.

The Alumni Relations office also facilitates communication between individual alumni, but in doing so does not release personal contact details without prior permission.

**Electronic Files**

DCUET and Alumni Relations office staff should not store data on the local drive of their computers or laptops. All documents must be stored on the DCU secure server.

Always keep passwords and usernames secure and do not share them. Always lock or log-off from your workstation when leaving it unattended and shut down at the end of the working day.

**Paper Files**

Hard copy data held in paper files should be kept in dedicated filing cabinets. Cabinets should be locked at the end of the working day and the keys held in a secure place. In addition offices should be locked when staff are absent and at the end of the day.
Summary of Responsibilities

DCUET Responsibilities

Key post holders have responsibility for ensuring that:

- All personal data being processed within DCUET complies with the Data Protection Acts and the DCUET’s Data Protection Policy.
- All contractors, agents and other non-permanent university staff used by DCUET are aware of and comply with, the Data Protection Acts and DCUET’s Data Protection Policy.
- All personal data held within DCUET is kept securely and is disposed of in a safe and secure manner when no longer needed.

Staff Responsibilities

All staff must ensure that:

- Personal data which they provide in connection with their employment is accurate and up-to-date, and that they inform DCUET of any errors, corrections or changes, for example, change of address, marital status, etc;
- Personal data relating to living individuals which they hold or process is kept securely;
- Personal data relating to living individuals is not disclosed either orally or in writing, accidentally or otherwise, to any unauthorised third party.
- When supervising temporary staff who are processing personal data, that those staff are aware of the Data Protection Rules, and DCUET’s Data Protection Policy.


The Data Subject is entitled to:

- Access to a copy of any data held by DCUET which relates to them;
- Require that any inaccurate data held by DCUET is corrected or erased;
- Prevent processing of the data likely to cause them distress or damage;
- Prevent evaluative decisions being made solely by automated means;
- Prevent processing of their personal data for the purposes of Direct Marketing;
- Request assistance from the Data Protection Commissioner’s Office;
- In the event of a breach of these rights, to pursue compensation through the Courts.

Subject Access Request (SAR)

A Data Subject is entitled to a copy of all data held by DCUET which relate to them. A fee for this service is allowed by the legislation and DCUET policy is to apply the fee.

To be a valid request, the SAR must be:

- Made in writing to the controller
- Provide adequate identification
On receipt of a valid SAR, DCUET must comply with the request as soon as possible, but within not more than 40 days from receipt of the request.

**Transfer of Data Overseas**

The Data Protection Acts prohibits the transfer of personal data to any country outside of:

- The European Economic Area (EEA = EU Member States plus Iceland, Liechtenstein and Norway);
- The 7 designated Safe Countries (Canada, Argentina, the Isle of Man, Guernsey, Jersey, the Faroe Islands and Switzerland)
- Organisations within the United States which subscribe to the ‘Safe Harbour’ principles.

Before transfer to any other destination, DCUET, as a Data Controller, must be satisfied as to the adequacy of protection which will be provided to the data at its destination.

**FOR FURTHER INFORMATION:**


This Policy document will be reviewed regularly and updated as appropriate in line with any legislative or other relevant development.
**Definitions**

**Data**

Information which is being used or held in a computerised system, or a ‘relevant filing system’ i.e. a manual filing system that is structured in such a way that data contained within it is readily accessible. Data can be written information, photographs, fingerprints or voice recordings.

**Personal Data**

Information that identifies and relates to a living individual, and includes any expression of opinion or intention about the individual. Personal data could be contact details, date of birth, qualifications, or anything pertaining to an individual. It is something that affects that person’s privacy (whether in their personal/family life, or business/professional capacity) in the sense that the information has the person as its focus or is otherwise biographical in nature, and identifies that person – by itself or with other information.

Personal data shall not be processed unless at least one of the following conditions is met:

- The consent of the individual.
- The performance of a contract with the individual.
- A requirement under a legal obligation.
- The protection of the individual’s vital interests.
- The processing is necessary -
  1. for the administration of justice,
  2. for the performance of a function conferred on a person by or under an enactment,
  3. for the performance of a function of the Government or a Minister of the Government,
  4. for the performance of any other function of a public nature performed in the public interest by a person,

The processing is necessary for the purposes of the legitimate interests pursued by DCUET or by a third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject.

**Sensitive Personal Data**

Sensitive personal data is defined as information relating to an individual’s:

- Racial or ethnic origin
- Political opinions
- Religious beliefs or beliefs of a similar nature
- Membership of a trade union
- Physical or mental health or condition
- Sexual life
. Commission or alleged commission of an offence
. Proceedings for any offence or alleged offence, or sentence of court

Processing

Anything which can be done with personal data i.e. obtaining, recording, holding, organising, adapting, altering, retrieving, consulting, disclosing, aligning, combining, blocking, erasing, destroying etc.

Data Subject

An individual who is the subject of personal data. This will include: staff, current and prospective students, graduates, business associates, conference delegates, survey respondents etc.

Data Controller

Refers to Dublin City University Educational Trust (DCUET). This includes university staff who collect and process personal data on behalf of DCUET, and students and temporary staff who are collecting and processing personal data on behalf of DCUET.

Data Processor

Any person (other than an employee of the DCUET) who processes personal data on behalf of DCUET, e.g. printing agency.

Recipient

Any person or organisation to which personal data is disclosed.

Document Change Management

Dublin City University Educational Trust believes that it is important to keep this Data Protection Policy current in order to ensure that it addresses legislative changes and security issues accurately, and is up-to-date with evolving business issues and technologies. This policy is a living document that will be reviewed annually and/or updated as needed.